

1 GREENBERG TRAURIG, LLP  
2 IAN C. BALLON (SBN 141819)  
3 WENDY M. MANTELL (SBN 225544)  
4 NINA D. BOYAJIAN (SBN 246415)  
5 2450 Colorado Avenue, Suite 400E  
6 Santa Monica, California 90404  
7 Telephone: (310) 586-7700  
8 Facsimile: (310) 586-7800  
9 Email: ballon@gtlaw.com, mantellw@gtlaw.com,  
10 boyajiann@gtlaw.com

11 Attorneys for Plaintiff  
12 MYSPACE, INC.

13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**UNITED STATES DISTRICT COURT**  
**CENTRAL DISTRICT OF CALIFORNIA**

MYSPACE, INC., a Delaware  
Corporation,

Plaintiff,

vs.

SANFORD WALLACE D/B/A  
FREEVEGASCLUBS.COM, REAL-  
VEGAS-SINS.COM, and FEEBLE  
MINDED PRODUCTIONS, an  
individual,

Defendant.

CASE NO. CV-07-1929 ABC (AGRx)

**SUPPLEMENTAL DECLARATION  
OF SARAH KALEEL IN SUPPORT  
OF MYSPACE, INC.'S REPLY TO  
OPPOSITION TO MOTION FOR  
PRELIMINARY INJUNCTION**

**Filed concurrently with:**  
**Myspace, Inc.'s Reply to Opposition  
to Motion For Preliminary Injunction  
Declaration of Aber Whitcomb  
Declaration of Allison Corona  
Declaration of Marco Hardi  
Objections to Evidence  
Responses to Evidentiary Objections**

DATE: July 2, 2007  
TIME: 10:00 a.m.  
JUDGE: Hon. Audrey B. Collins  
CRTRM: 680

**SUPPLEMENTAL DECLARATION OF SARAH KALEEL**

I, Sarah Kaleel, do declare:

1. I am the Director of Policy Enforcement for MySpace, Inc. ("MySpace"), located in Beverly Hills, California. The following facts are known by me to be true and correct and if called as a witness I could and would competently testify thereto under oath.

2. I have reviewed Mr. Wallace's Declaration in support of his Opposition to MySpace's Motion for Preliminary Injunction and disagree with many of Mr. Wallace's contentions.

3. Mr. Wallace states in paragraph 3 of his declaration that his websites are "two of the many on the internet that offer tell-a-friend services through MySpace." Mr. Wallace's "tell-a-friend" services are not designed as legitimate services. In my experience, a legitimate "tell-a-friend" service would never ask for a user's login credentials, such as a password, in order to share something with friends. MySpace does not permit any "tell-a-friend" services on the Internet to gather MySpace usernames and passwords, and in fact such conduct is expressly prohibited in MySpace's Terms of Use Contract. *See* Declaration of Sarah Kaleel in Support of MySpace's Motion for Preliminary Injunction ("Kaleel Declaration"), Exh. B, p. 9 (§ 5), Exh. C, p. 17 (§ 5).

4. Mr. Wallace claims in paragraph 9 of his declaration that he "did not use and is unaware of any software or bot that can automatically read MySpace verification code characters." Notably, Mr. Wallace does not deny that he used a script or bot to enter all of the information necessary to create a MySpace account other than the verification code (*See* Kaleel Declaration, Exh. A, p. 6), nor does Mr. Wallace deny using a script or bot to send out mail messages on MySpace.com. As explained in the Kaleel Declaration, the number of MySpace profiles Mr. Wallace created, along with the consistency in the naming conventions of the display names and the alternate email addresses used to acquire those profiles make it highly unlikely that a human created the accounts with no assistance from an automated script. Mr. Wallace could have used an automated script or

1 bot to accomplish all of the steps of the MySpace signup process prior to having to enter  
2 the verification code, which is merely the final step of the process.

3 5. Mr. Wallace claims in paragraph 10 of his declaration that all of his "access  
4 to MySpace has originated from the same few IP addresses which easily could be  
5 blocked by MySpace." As a general policy, MySpace does not block Internet Protocol,  
6 ("IP") addresses because blocking IP addresses can affect innocent users' access to  
7 MySpace. Additionally, blocking IP addresses is not an effective method of combating  
8 abusive behavior on MySpace because it is easy for users to change their IP addresses  
9 when a particular IP address is blocked.

10 6. Mr. Wallace claims that MySpace can block the URLs he includes within  
11 his messages. While it is true that MySpace can block messages containing particular  
12 URLs, the Abuse Team has thus far discovered that Mr. Wallace has used at least 25  
13 different URLs in his attacks on MySpace.com. Therefore, it would be futile for  
14 MySpace to block any of the URLs Wallace includes in his attacks, since he would  
15 simply be able to change the URL in subsequent attacks.

16 7. Mr. Wallace also claims that while the URLs he uses in his spam messages  
17 are for websites he controls, those websites are not the two websites "at issue in this  
18 case." The particular URLs Mr. Wallace uses in his spam messages contain links with  
19 addresses containing domain names for websites other than freevegasclubs.com and real-  
20 vegas-sins.com (such as the ploppityeeekoneeko.com URL used in the attack described  
21 below); however, all of the links are configured so that when clicked on, they redirect  
22 users to pages of the real-vegas-sins.com or freevegasclubs.com websites. Hence, Mr.  
23 Wallace's contention that the links he includes within his spam messages are to websites  
24 that he controls, but are "not the two at issue here," is inaccurate.

25 8. As stated in the Declaration of Allison Corona, the MySpace Abuse Team  
26 received at least 831 complaints from MySpace users relating to Mr. Wallace's activity  
27 on MySpace.com. In my experience as the Director of the MySpace Abuse Team, this is  
28 a significant number of complaints related to a single attacker.

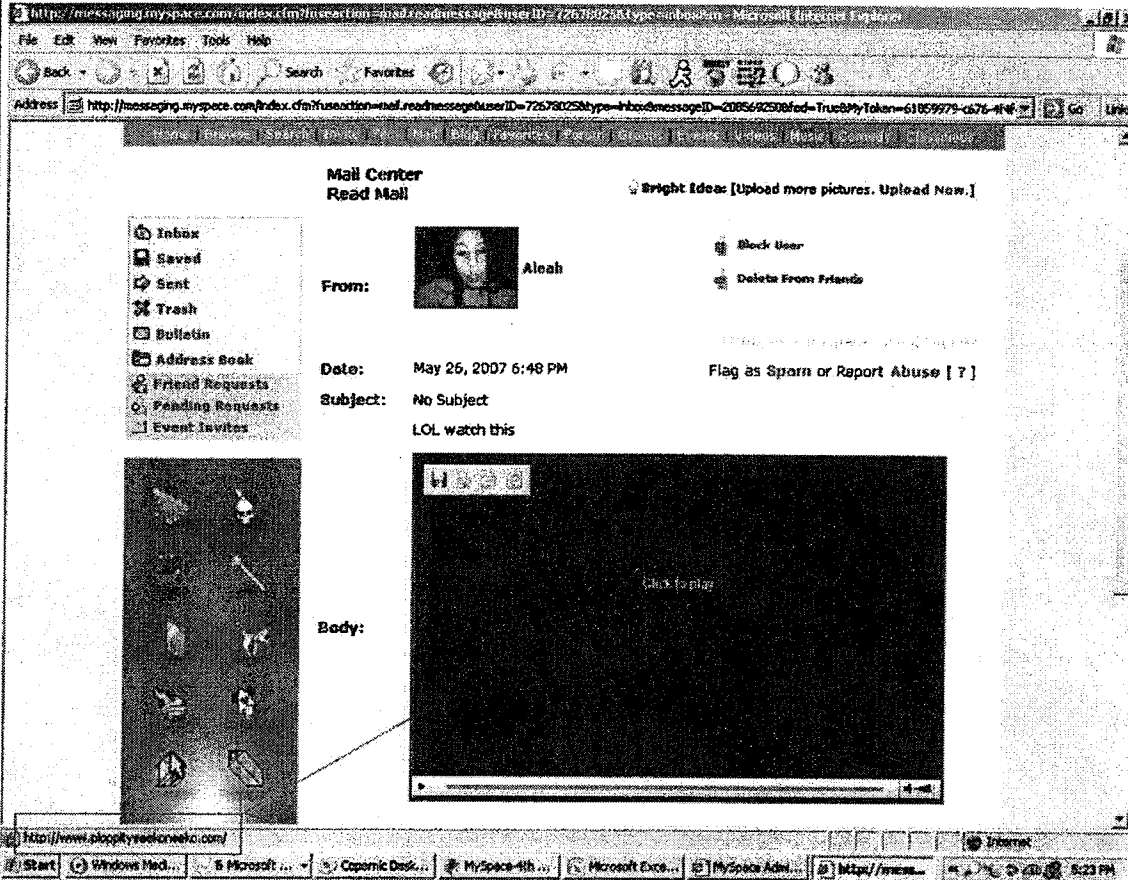
1           9.     The MySpace Abuse team does not know about spamming, phishing and  
2 other attacks on MySpace the moment they occur. MySpace has over 180 million  
3 registered members, and it would be impossible to monitor every MySpace email account  
4 every day. MySpace relies on user complaints, and database monitoring to discover large  
5 scale spamming, phishing, and other attacks on MySpace.com. Once a member of the  
6 MySpace Abuse Team receives a user complaint about spamming, phishing, or other  
7 attacks on MySpace.com, it also takes time for the Abuse Team to escalate the  
8 investigation process, and to work with the database administrators to gather evidence of  
9 the attacks before passing the information on to MySpace's legal team. Because of the  
10 size of the MySpace databases, it will often take the Abuse Team weeks or months to  
11 gather evidence of a spamming, phishing, hacking, or other attack on MySpace.com  
12 before MySpace is able to take any legal or other action against the spammer, phisher, or  
13 hacker.

14           10.    For example, between the time that I signed a declaration in support of  
15 MySpace's Motion for Preliminary Injunction and the date of this declaration, the  
16 MySpace Abuse Team uncovered another attack on MySpace launched by the defendant,  
17 Sanford Wallace. This attack was not uncovered previously because Mr. Wallace used a  
18 different URL in the body of the spam messages he sent from MySpace user accounts  
19 than the URLs he had used in the previous attacks; however, because the URL redirected  
20 users to Mr. Wallace's website, [www.real-vegas-sins.com](http://www.real-vegas-sins.com), and because the anatomy of  
21 the attack is exactly the same as that of the other attacks described in the Declaration of  
22 Rick Frazier in support of MySpace's Motion for Preliminary Injunction ("Frazier  
23 Dec."), it appears that this latest attack was also launched by Mr. Wallace.

24           11.    Starting on approximately May 10, 2007 through at least June 14, 2007,  
25 more than 110,000 email messages were sent using at least 76,200 legitimate MySpace  
26 user accounts without authorization through the MySpace email servers. The subject line  
27 of the message was: "LOL watch this" and the body of the message contained the  
28

following code: "Body:<br><br><a href="http://www.ploppityeeekoneeko.com"></a>."

The messages included an image embedded that made it look like the user was recommending a video. The messages looked like this:



The image was actually a simple graphic made to look like a video player, but was wrapped by a clickable link to "ploppityeeekoneeko.com", which when clicked, automatically redirected a user to <http://94377597.real-vegas-sins.com/video/login.html>. Below is a screenshot of the page to which users were automatically redirected when they clicked on the <http://pic.ploppityeeekoneeko.com/clicktoplay.jpg> link:



1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16

File Edit View Favorites Tools Help

Back Forward Stop Reload Home Search Favorites

Address http://94377597.real-vegas-sins.com/video/login.html

**Must authorize below to view video**

To view video, you must be a member of either

[FreeRing Network \(16+\)](#)

or

[Fling \(18+\)](#)

Alternatively, you may qualify for temporary access below.  
(note that Fling and FreeRing members receive permanent free access to this area)

Use your current email/password  
as temporary registration.

Login Info:

E-Mail:

Password:

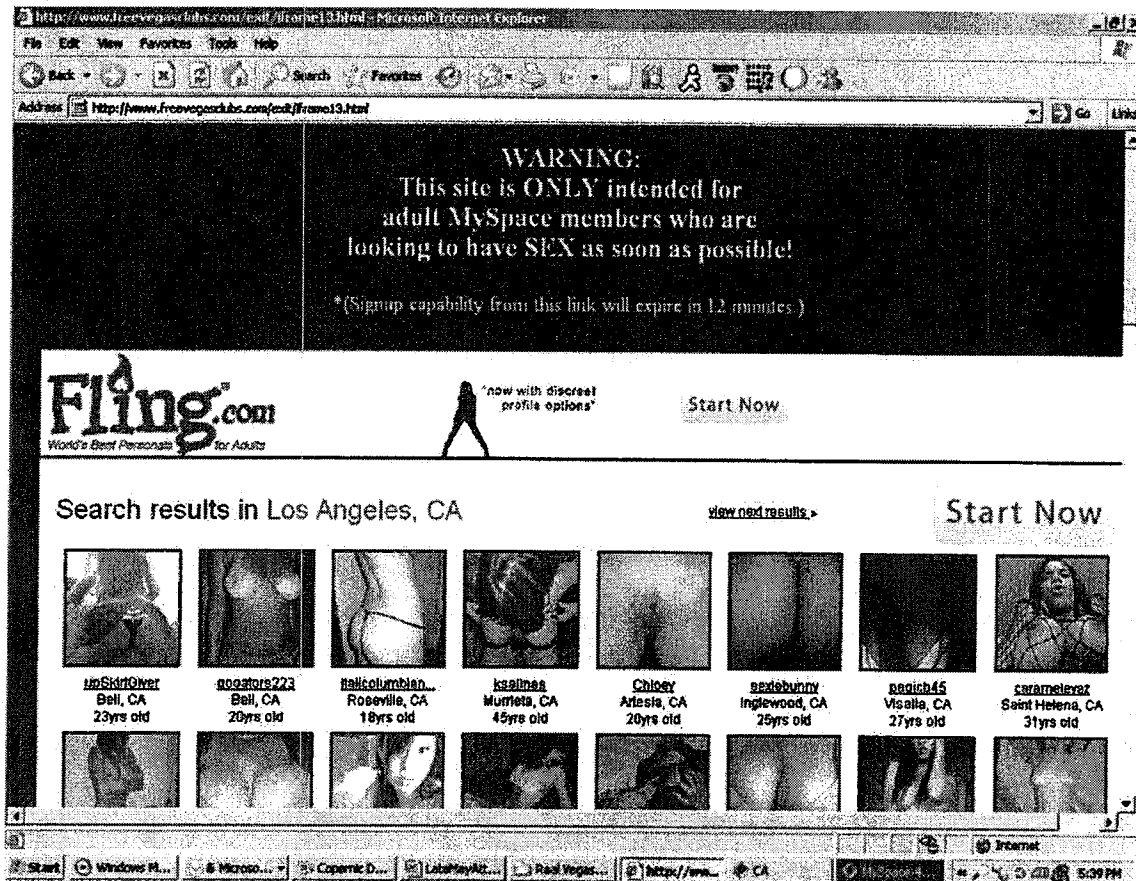
17  
18  
19  
20  
21  
22  
23  
24  
25  
26

This page asked for users' login information, and did not contain any terms of use or disclosures. Once users hit submit on this page, the sequence of the attack continued in the same manner as Mr. Wallace's other attacks on MySpace, described in the Frazier Declaration at paragraph 8. Mr. Wallace used the exact same mouse-trapping techniques as were used in his earlier-described attacks, and again when users tried to close his webpages, a series of popup messages were displayed with various information or questions, all designed to redirect users to Mr. Wallace's websites, or those of his affiliates. Clicking through the series of popups, users were eventually redirected to either webpage advertisements or adult content websites.

27  
28

12. The MySpace Abuse recently uncovered another attack on MySpace that promotes the adult content website [www.Fling.com](http://www.Fling.com), using a link to one of the websites admittedly owned and operated by Sanford Wallace, [freevegasclubs.com](http://freevegasclubs.com). The MySpace

Abuse Team is still gathering evidence of this attack. What is known thus far is that approximately 400 MySpace profiles and corresponding email accounts were created by the same IP address (82.71.5.17) promoting the URL "ultra.themusthaveme.com" in the profile's About Me section. When users click on the link, they are redirected to www.freevegasclubs.com/exit/frame13.html. This is a website that uses frames to mask the real site embedded in the page, which is http://www.fling.com/enter.php?prg=1&t=best&id=magic3937. The link brings you to the following page containing adult content, with no age verification:



When a user is brought to this page, an audio file plays simultaneously that says "LET'S FUCK."

1 I declare under penalty of perjury under the laws of the State of California that the  
2 foregoing is true and correct and that this Declaration was executed this 25 day of June,  
3 2007 at Beverly Hills, California.  
4

5   
6

7 Sarah Kaleel  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28